

Chairwoman Mikie Sherrill (D-NJ) of the Subcommittee on Investigations and Oversight

Subcommittee on Investigations and Oversight Hearing:

Online Imposters and Disinformation

Thursday, September 26, 2019

Good morning and welcome to a hearing of the Investigations & Oversight Subcommittee.

We're here today to discuss online imposters and disinformation. Researchers generally define *misinformation* as information that is false but promulgated with sincerity by a person who believes it is true. *Disinformation*, on the other hand, is shared with the deliberate intent to deceive.

It turns out that these days, the concepts of disinformation and online imposters are almost one and the same. We all remember the classic scams and hoaxes from the early days of email – a Nigerian Prince needs help getting money out of the country! But today, the more common brand of disinformation is not simply content that is plainly counterfactual, but that it is being delivered by someone who is not who they say they are.

We are seeing a surge in coordinated disinformation efforts particularly around politicians, hotbutton political issues, and democratic elections. The 2016 election cycle saw Russian troll farms interfering in the American discourse across Facebook, Twitter, Instagram, Youtube and beyond, trying to sway public opinion for their preferred candidate. But at the same time, they were after something else much simpler: to create chaos. By driving a wedge into the social fissures in our society, sowing seeds of mistrust about our friends and neighbors, exploiting social discord, they think they might destabilize our democracy and allow the oligarchy to look a little more attractive by comparison. When I was a Russian policy officer in the Navy, I learned how central information warfare is in Russia's quest to dominate western nations. And unfortunately, modern technology makes information warfare a far easier proposition for our antagonists, foreign or domestic.

In fact, its perhaps too easy today to proliferate convincing, harmful disinformation, build realistic renderings of people in videos, and impersonate others online. That's why the incidence of harmful episodes has exploded in the last few years. They range from fake reviewers misleading consumers on Amazon, to impersonating real political candidates, to fake pornography being created with the likenesses of real people. Earlier this year, an alleged

deepfake of the President of Gabon helped trigger an unsuccessful coup of the incumbent government. Deep fakes are particularly prone to being weaponized, as our very biology tells us that we can trust our eyes and ears.

There are social science reasons why disinformation and online imposters are such a confounding challenge: research has shown that online hoaxes spread six times as fast as true stories, for example. Maybe human nature just likes a good scandal. And confirmation bias shapes how we receive information every time we log on or open an app. If we encounter a story, a video or an influence campaign that seems a little less than authentic, we may still be inclined to believe it if the content supports the political narrative already playing in our own heads. Our digital antagonists, whether the intelligence service of a foreign adversary or a lone wolf propagandist working from a laptop, know how to exploit all of this.

Our meeting today is the start of a conversation. Before we as policymakers can address the threat of fake news and online frauds, we have to understand how they operate, the tools we have today to address them, and where the next generation of bad actors is headed. We need to know where to commit more resources in the way of innovation and education.

Our distinguished witnesses on today's panel are experts in the technologies that can be used to detect deep fakes and disinformation, and I'm glad they are here to help us explore these important issues. We are especially thankful that all three of you were able to roll with the punches when we had to move the hearing due to a change in the Congressional schedule.

I'd also like to thank my Republican counterparts who have been such great partners on this matter. Mr. Gonzalez of Ohio is joining us today to inform his work on deep fakes. I'm proud to be a cosponsor of his bill H.R. 4355, and I thank you for being here, Mr. Gonzalez.